Privacy Policy

Current from 4 November 2026

At Traditional Credit Union Limited (TCU, 'we', 'us', 'our'), we value your trust as a member-owned bank. We understand how important it is to protect your privacy and the security of your personal information. We are committed to treating your information with care and confidentiality.
We comply with the Privacy Act 1988 (Cth), including the Australian Privacy Principles and Part IIIA, and the Privacy (Credit Reporting) Code 2025, as amended or replaced from time to time.
This Privacy Policy outlines how we collect, use, disclose and store your personal information, and explains your rights under the law. If we have a separate agreement with you that provides for different arrangements, the terms of that arrangement will apply to the extent of any inconsistency.

Although the Consumer Data Right (CDR) regime allows consumers to authorise the sharing of their data between financial service providers, TCU is currently exempt from participation in the CDR scheme. While this exemption is in place, we are unable to support CDR data-sharing requests. You can still access your information by contacting us directly.

TCU provides a range of banking products and services. To deliver these effectively and meet our legal obligations, we need to collect certain personal information from you.

Key types of information

Certain words have special meanings when used in this Policy. These are shown below.

"Personal information" means information or an opinion about an identified individual or an individual who is reasonably identifiable. Although we try to make sure that all information we hold is accurate, "personal information" also includes any inaccurate information about an individual. In this policy 'personal information' includes "Credit-related information" (as below) unless otherwise specified.

"Credit eligibility information" means information that has been obtained from a credit reporting body, or that has been derived from that information, that is about an individual's credit worthiness.

"Credit information" means personal information that includes the following:

- information about an individual, like their name, age, address and employment details, that we may use to identify that individual;
- information about an individual's current or terminated consumer credit accounts and their repayment history, or that the individual has agreed to be a guarantor;
- financial hardship information;
- the type and amount of credit applied for in any previous consumer or commercial credit applications to any credit provider, where that credit provider has requested information;
- information about an individual from a credit reporting body;
- information about consumer credit payments overdue for at least 60 days and for which collection action has started;
- advice that payments that were previously notified to a credit reporting body as overdue are no longer overdue;
- information about new credit arrangements an individual may have made with a credit provider, in relation to consumer credit currently or previously held, to deal with any defaults or serious credit infringements by that individual;
- information about court judgments which relate to credit that an individual has obtained or applied for;
- information about an individual on the National Personal Insolvency Index;
- publicly available information about an individual's credit worthiness; and
- an opinion of a credit provider that an individual has committed a serious credit infringement of credit provided by that credit provider.

We may not hold all of these kinds of information about a particular individual. However, if we hold any of these kinds of information, it is protected as "credit information" under this Policy.

"Credit-related information" means credit information, credit eligibility information and related information.

How we collect your information

We will primarily collect personal information about you directly from you or via a method authorised by you (e.g. in an application, over the telephone, face to face, through mobile banking app, social media or our website). Wherever possible, this information will generally come from what you provide in relation to an application for membership and/or for our products or services and supporting documentation.

We only ask for personal information relevant to our business relationship with you. When you apply for one of our products or services, we may request:

- Identification information and contact details
- Information about your job, income, assets, and debts
- Your tax file number or tax identification number if you are a foreign resident
- The purpose for which you intend to use the product or service; and
- Any other information we are required or authorised to collect by law

Your image may also be captured through security cameras located in our branch locations. These images are secure and are destroyed when no longer needed.

In some circumstances, we may collect personal information about you from third parties, such as any referees that you provide, your employer, other credit providers, credit reporting bodies, and through your interactions with us via social media platforms and digital communication channels.

Credit reporting bodies collect credit information about individuals which they provide as credit reports to credit

providers and others in the credit industry to assist them in managing credit risk, collecting debts and other activities. You can also ask a credit reporting body, through contact details on their website, not to use or disclose your personal information if you believe on reasonable grounds that you have been or are likely to be a victim of fraud, including identity fraud.

Some information is created through our internal processes, like credit eligibility scoring information.

How we use your personal information

We may use your personal information for the purpose of providing products and services to you and managing our business. This may include:

- assessing and processing your application for the products and services we offer;
- establishing and providing our systems and processes to provide our products and services to you;
- executing your instructions;
- charging and billing;
- uses required or authorised by law;
- maintaining and developing our business systems and infrastructure;
- research and development;
- monitoring transactions and account activity to detect and prevent fraud, scams and unauthorised access;
- collecting overdue payments due under our credit products;
- managing our rights and obligations regarding external payment systems; and
- marketing, including direct marketing.

We do not use or disclose your personal information (including credit-related information) for a purpose other than:

- a purpose set out in this Policy;
- a purpose you would reasonably expect;
- a purpose required or permitted by law; or
- a purpose otherwise disclosed to you, or a purpose requested by you and to which you have consented.

Automated decision-making

We use computer programs, including systems provided by our service providers, to make some decisions automatically and to help our staff make others. This section explains the kinds of personal information these programs use and the kinds of decisions they make or help with.

Personal information we use

Depending on the decision, these programs may use:

- your identification and contact details;
- your account, card, transaction and payment details, including who you pay and who pays you;
- how you access our services, such as device, login and IP address details, and location details for card transactions;
- information you give us when you apply for a loan, such as your income, expenses, assets and debts;
- credit information and credit eligibility information, including credit scores from credit reporting bodies;
- the results of identity checks and of screening against sanctions, politically exposed person and other watch lists; and
- information you give us when you apply for a job with us.

Decisions made by computer programs alone

To protect you and TCU from fraud, scams and unauthorised access, and to run your accounts, our systems may automatically:

- hold, delay or stop a transaction or payment that breaches our fraud monitoring rules or appears to be high risk;
- decline a card transaction in real time for the same reasons;
- lock your access to internet banking or our app after too many failed login attempts;
- decline or dishonour a payment or direct debit when there are not enough funds in your account; and
- pause a membership or account application until a staff member has reviewed the results of identity verification or screening.

A staff member can review any of these decisions. If you think a decision is wrong, please contact us.

Decisions where computer programs help our staff

Computer programs also produce calculations, scores, alerts or matches that our staff rely on when deciding:

- whether to approve a personal loan and how much we can lend, using a serviceability calculation and your credit score;
- whether to accept your membership or open an account, using identity verification and screening results;
- whether to release a held transaction or remove a restriction;
- what action to take on alerts from our transaction monitoring system, as required under anti-money laundering and counter-terrorism financing laws; and
- whether to shortlist a job applicant.

In these cases, a staff member considers the result and makes the final decision.

We do not use artificial intelligence tools to make decisions about members.

How we disclose your personal information

- We may disclose your personal information to other organisations, for example: external organisations that are our assignees, agents or contractors;
- external service providers to us, such as organisations which we use to verify your identity, payment systems operators, mailing houses and research consultants;
- other financial institutions, for example, when you apply for a loan from another credit provider and you agree to us providing information;
- credit reporting bodies, including disclosing that you are in default under a credit agreement or commit a serious credit infringement, if that is the case;
- debt collecting agencies, if you have not repaid a loan as required;
- our professional advisors, such as accountants, lawyers and auditors;
- certain entities that have bought or otherwise obtained an interest in your credit product, or that are considering doing so, and their professional advisors;
- any organisation with which we are considering merging;
- your representative, for example, lawyer, mortgage broker, financial advisor or attorney, as authorised by you; or
- if required or authorised by law, to government and regulatory authorities.

We will take reasonable steps to ensure that these organisations are bound by sufficient confidentiality and privacy obligations with respect to the protection of your personal information. TCU does not disclose personal information to overseas recipients. We periodically verify this position against our service-provider, technology-support and data-hosting arrangements and will update this Policy if that position changes. We may also disclose your personal information to an individual or an organisation (a 'third party') if:

- you direct us to do so;
- you consent to the third party obtaining the information from us; or
- you consent to the third party accessing the information on our systems, and/or do anything which enables the third party to obtain access.

Your consent to a third party obtaining or accessing information may be implied from:

- your use of any service or application which a third party provides to you, or makes available to you, which involves the third party obtaining or accessing personal information held by us or organisations like us; or
- you doing anything else which enables the third party to obtain access to the information.

Sensitive information

Sensitive information includes information about an individual's health, membership of a professional or trade association, biometrics and racial or ethnic origin. We may collect information about a person's Aboriginal or Torres Strait Islander status where it is reasonably necessary for our functions or activities, including understanding and serving our members and communities.

We collect sensitive information only where you have consented and the information is reasonably necessary for one or more of our functions or activities, or where the collection is otherwise required or authorised by law. We will explain why the information is required when seeking your consent.

Refusal of credit applications

We may refuse an application for consumer credit made by you individually or with other applicants. Our refusal may be based on credit eligibility information obtained from a credit reporting body about either you or a co-borrower. In that case, we will give you written notice that the application has been refused on the basis of that information. We will tell you the name and contact details of the relevant credit reporting body and other relevant information.

Keeping your information secure

We take all reasonable steps including technical and organisational measures, to ensure that your personal information held on our website or otherwise is protected from:

- misuse, interference and loss; and
- unauthorised access, disclosure or modification.

Your personal information may be held by us in paper or electronic form. All personal information is stored within secure systems which are in controlled facilities. There are restrictions on who may access personal information and for what purposes. Our employees, contractors, service providers and authorised agents are obliged to respect the confidentiality of personal information held by us.

If we suspect or believe that there has been any unauthorised access to, disclosure of, or loss of, personal information held by us, we will promptly investigate the matter and take appropriate action, and we will comply with any obligations in relation to notifiable data breaches that are in force under the Privacy Act.

We ask you to keep your passwords, personal identification numbers, and tokens and other authentication devices safe, in accordance with our suggestions.

You can also help to keep the personal information that we hold about you secure by taking care before you authorise or otherwise assist any third party to obtain or gain access to that information (see 'How we disclose your personal information' above). You should never provide or disclose any of your passwords or personal identification numbers to any third party to enable the third party to obtain or access to your personal information. If you do, you may breach the ePayments Code and the terms and conditions applying to the products and services we provide to you and you may be liable for any unauthorised transactions that subsequently occur.

When we no longer require your personal information (including when we are no longer required by law to keep records relating to you), we take reasonable steps to ensure that it is destroyed or de-identified.

Website and Apps

This section explains how we handle personal information collected from our website and our app. If you have any questions or concerns about transmitting your personal information via the internet, you may contact us using the details in the Privacy Questions and Complaints section of this Policy, as there are other ways for you to provide us with your personal information.

(a) Visiting our website - Anytime you access an unsecured part of our website, that is, a public page that does not require you to log on, we will collect information about your visit, such as:

- the time and date of the visit;
- any information or documentation that you download;
- your browser type; and
- internet protocol details of the device used to access the site.
- We also know that some customers like to engage with us through social media channels. We may collect information about you when you interact with us through these channels. However, for all confidential matters, we'll ensure we interact with you via a secure forum.

(b) Cookies - A "cookie" is a small text file which is placed on your internet browser and which we may access each time you visit our website. When you visit the secured pages of our website (i.e. pages that you have to provide login details to access) we use cookies for security and personalisation purposes. When you visit the unsecured pages of our website (i.e. public pages that you can access without providing login details) we use cookies to obtain information about how our website is being used. You may change the settings on your browser to reject cookies, however doing so might prevent you from accessing the secured pages of our website.

(c) Email - When we receive emails, we will retain the content of the email and our response to you where we consider it necessary to do so. Your email address, provided by you when you send us an email, will only be used, or disclosed for the purpose for which it was provided. It will not be added to any

mailing lists or used for any other purpose without your consent.

(d) Security - We use up-to-date security measures on our website to protect your personal information. Any data containing personal, credit or related information which we transmit via the internet is encrypted. However, we cannot guarantee that any information transmitted via the internet by us, or yourself, is entirely secure. You use our website at your own risk.

(e) Links on our website - Our website may contain links to third party websites. The terms of this Policy do not apply to external websites. If you wish to find out how any third parties handle your personal information, you will need to obtain a copy of their privacy policy.

(f) Our app - If you use fingerprint or face recognition to log in to our app, the check is done on your own device. We do not receive or store your fingerprint or facial information.

Access or correcting your personal information

You can request access to the personal information we hold about you at any time, or ask us to correct it if it's inaccurate, incomplete, or out of date. We may need to confirm your identity before processing your request. If the information is easily accessible, we'll provide it straight away. Otherwise, we'll respond within a reasonable time. Access to your personal information is generally free of charge. In limited cases, where retrieval involves significant resources, a reasonable fee may apply (see our Interest, Fees and Charges Brochure).

In rare cases, we may refuse access as allowed under the Privacy Act 1988. If this happens, we'll explain why and how you can challenge the decision.

Marketing

Where we are permitted to do so by law, we may use your personal information, including your contact details, to provide you with information about products and services, including those of other organisations, which we consider may be of interest to you. These communications may be made by telephone, email, SMS, post or another appropriate channel.

Before using a particular channel, we will ensure that the communication is permitted by applicable privacy, spam and telephone marketing laws. We will respect your communication preferences and any applicable requirements of the Do Not Call Register. You may request, at any time, not to receive marketing communications or not to receive them through a particular channel. We will provide a simple way to opt out and will act on your request within the timeframe required by law. Opting out will not prevent us from sending account information, security and fraud alerts, required notices or other communications that are not marketing.

Unless we have first obtained your consent, we will not provide your personal information to other organisations to use for their marketing purposes.

Changes to the Privacy Policy

We may make changes to this Policy from time to time (without notice to you) that are necessary for our business requirements or the law. Our current Policy is available on our website at **https://tcu.com.au/privacy-policy-2/** and at any of our branches.

Privacy Questions and Complaints

If you have any questions or concerns about this Policy or how we handle your personal information, please contact us. This includes where you believe your privacy has been compromised or your information is not being adequately protected, or you have concerns about a decision made or assisted by a computer program.

You can raise a complaint with us if you think we have breached the APPs, the Privacy Act 1988, the Privacy (Credit Reporting) Code 2025, or any credit reporting obligations.

You can contact us:

- In person: 9 Rowling Street, Casuarina NT 0810 or at one of our remote branch locations
- By post: PO Box 40425, Casuarina NT 0811
- By phone: 08 8999 0777
- By email: info@tcu.com.au

We handle your concern or complaint in line with our **Complaints Handling – Member Policy** (available on our website Complaint-Handling-Member-Policy-v2-June-2025-Public-Website.pdf). Our aim is to resolve your issue as quickly and fairly as possible, ideally at the first point of contact. If we need more time, we will let you know the reason and seek any consent required by law. If you are not satisfied with our initial response, we will escalate the matter for further review.

If you remain dissatisfied after this, you may contact one of the following external bodies:

Australian Financial Complaints Authority
Post: GPO Box 3 Melbourne VIC 3001
Telephone: 1800 931 678
Website: www.afca.org.au

Office of the Australian Information Commissioner
Post: GPO Box 5218 Sydney NSW 2001
Telephone: 1300 363 992
Website: www.oaic.gov.au